Cyber Patrol: Careless keyboards can kill

By Ed Beemer
January 24, 2006

ARLINGTON, Va. (Army News Service, Jan. 24, 2006) -- Fewer people would know about a deployment or operation if you screamed it out at the Superbowl than if you posted it on a Web log or blog.

Common sense will tell you not to discuss sensitive subjects on the streets of Baghdad. The same common sense should apply on the highways of cyberspace. Soldiers need to keep this in mind, not only because it is the right thing to do, but because it could land them in a world of trouble.

The technology of communication is a double-edged sword and often the sharper edge is being used against you. There have been too many instances of sensitive information being made public. For example one officer posted a picture of his tactical operations center or TOC, complete with secret documents showing troop rotations.

Another Soldier in theater posted when his unit's laundry runs were. That information has IED opportunity written all over it.

The list of what should not be posted on an unsecured site or sent via unsecured communication channels is almost endless. It includes the obvious like troop movements, operational details, TDYs, planning issues and any classified material. But it also includes any personal information – information that could be used to put you, your fellow soldiers or even your own family at risk.

This is also a matter of situational awareness; knowing what seemingly innocent information could be useful to the enemy. Each unit's operational security professional needs to advise supervisors on means to prevent the release of sensitive information.

But every Soldier, regardless of rank and position, has a personal responsibility to safeguard what makes it onto the Internet. In order to ensure that sensitive and unauthorized information is not posted, check with your immediate supervisor for approval before your next blog entry or site update. More information on OPSEC can be found at https://opsec.1stiocmd.army.mil/io_portal/Public/Pages/Sections.cfm?Section=Opsec

This is a very serious matter and the fallout from even one instance of releasing unauthorized information can be severe. Senior Army commanders have clearly stated that the Army must "hold people accountable that place others at risk."

Relevant punitive measures are spelled out in AR 25-2 and are worth a thorough reading.

Soldiers have been fined and demoted because of information put on a blog that could have helped the enemy. But the consequences of allowing mission and personal information to get out is more dangerous than simply running the risk of a fine; It could get your fellow Soldiers

killed and even put your family members in harm’s way.

Psychologically, keeping information tightly guarded is a challenge, especially for soldiers in a wartime environment a long way from friends and family. There is a great urge to connect and let people know what is going on.

Often it seems that just a little bit of information can’t hurt. Everyone needs to remember that there are many ears and eyes focusing on these little pieces of information.

A terrorist manual found in Afghanistan stated, 80 percent of information gathered on the enemy (you) is gathered openly! The technical abilities, resourcefulness, patience and determination of enemy operatives cannot be underestimated –watch what you blog!

(Editor’s note: Information provided by the G6 Information Assurance Office.)